WHAT IS CLAIMED IS

1. A method for securing, using and transferrring sensitive information, comprising the steps of:

calculating a digital signature for a file;

storing the digital signature within the file;

encrypting the file including the digital signature; and

performing a file input-output operation on a proper subset of the file, in a manner that permits such input-output operation without the need to decrypt the entire file.

2. The method of claim 1, wherein the step of performing a file input-output operation on the file further comprises:

inputting a data subset from a file stream; and

decrypting the data subset in a local function.

3. The method of claim 2, further comprising the step of:

updating the digital signature using the data subset input from the file stream and a data subset to be written to the file.

4. The method of claim 3, further comprising the steps of:

encrypting the data subset to be written to the file in a local function to produce an encrypted data subset to be written; and

writing the encrypted data subset to be written to the file.

5. The method of claim 4, wherein the step of performing file input-output operation on the file further comprises:

authenticating the file using the digital signature.

6. The method of claim 5, wherein the step of performing file input-output operation on the file further comprises:

authenticating the file using the user signature.

7. The method of claim 1, wherein the step of performing a file input-output operation comprises:

inputing a data subset from an encrypted, temporary copy of the file; and

decrypting the data subset in a local function to produce an unencrypted data subset read from the temporary, encrypted file.

8. The method of claim 7, further comprising the steps of:

updating the digital signature using the data subset input from the encrypted, temporary copy of the file and a data subset to be written to the file;

encrypting the data subset to be written to the encrypted, temporary file in a local function; and

writing the data subset to be written to the encrypted, temporary file.

9. The method of claim 9, further comprising the steps of:

copying the digital signature in memory to the encrypted, temporary file; and

copying the encrypted, temporary file to the file; and

closing the file.

10. The method of claim 7, further comprising the steps of :

authenticating the file using the digital signature.

11. The method of claim 10, further comprising the steps of:

authenticating the file using the user signature.

12. A machine readable medium comprising computer code, wherein the computer code further comprises:

a first function for reading an encrypted file with an encrypted digital signature; and

a second function for writing to an encrypted file with an encrypted digital signature; and

wherein the first and second functions do not require decryption of the entier file.

13. The machine readable medium of claim 12, wherein the computer code further comprises:

a third function for opening a file, wherein the third function is capable of authenticating a file with an encrypted digital signature.

14. The machine readable medium of claim 13, wherein the third function further comprises:

code for creating a temporary, encrypted file and generating a file stream therefrom.

15. The machine readable medium of claim 14, wherein the computer code further comprises:

code for implementing a digital signature using an symmetric, invertible function.

16. The machine readable medium of claim 15, wherein the computer code further comprises:

code for implementing a user signature within the file for authentication purposes.

17. The machine readable medium of claim 16, wherein the computer code further comprises:

a source code library of functions, implemented such that encryption, decryption and authentication a transparent to a source code programmer.

18. The machine readable medium of claim 16, wherein the computer code is executed in the same address space as a user application.

19. The machine readable medium of claim 16, wherein the computer code further comprises a database library using said first and second functions.

20. A method for managing sensitive data, comprising:

storing the sensitive data in an encrypted file with an encrypted digital signature and an encrypted user signature; and

storing a temporary, encrypted copy of the file;

decrypting a proper subset of the temporary, encrypted copy of the file in a function local to a trusted application when performing a read operation; and

decrypting a proper subset of the temporary, encrypted copy of the file in a function local to a trusted application when performing a write operation;

updating the digital signature of the encrypted, temporary file, using the proper subset and a data subset to be written to the encrypted, temporary file;

encrypting the data subset to be written to the temporary, encrypted file and writing said data subset to the temporary, encrypted file;

using the encrypted digital signature and encrypted user signature to authenticate the encrypted, temporary copy of the file; and

updating the file with the encrypted, temporary copy of the file when performing a file close operation.